CLAIM LISTING

Amendments to the Claims:

This listing of claims will replace all prior versions, and listing, of claims in the application:

Applicant has made a good faith effort to list each and every prior claim, including any amendments or changes thereto (or status thereof) in this "Listing" section, however, should there be any discrepancy between the previous version of a claim (or status thereof) and the listing not explicitly amended, canceled or otherwise changed by this amendment, only the previous version (and status thereof) should be referred to as the intent of the Applicant.

Listing of the Claims:

---

a'

1. (Amended) A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network, the method comprising the steps of:

determining whether the addressee has a public key;

in response to the addressee not having a public key:

encrypting the package with an escrow encryption key;

storing the package in escrow for the addressee;

notifying the addressee of the package in escrow; and

in response to receiving an acknowledgement from the addressee:

issuing new public and private keys to the addressee; and

in response to subsequently verified authentication of the addressee:

transmitting the package to the addressee via the network.

2. (Original) The method of claim 1, wherein the step of determining whether the addressee has a public key comprises the sub-step of:

checking a public key directory for a public key of the addressee.

3. (Original) The method of claim 1, further comprising the step of:

storing the addressee's new public key in a public key directory.

4. (Original) The method of claim 1, wherein the encrypting step comprises the sub-steps of:

providing an escrow encryption key and an escrow decryption key,

wherein the escrow encryption and decryption keys comprise one of symmetric keys and asymmetric keys; and

encrypting the package with the escrow encryption key.

5. (Amended) The method of claim 1, wherein the notifying step comprises the sub-step of:

sending a notification to the addressee via the network, wherein said notification includes an attached module for generating private and public keys at the addressee location.

6. (Original) The method of claim 5, wherein the notification comprises one of an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification.

7. (Original) The method of claim 1, further comprising the step of:

decrypting the package with an escrow decryption key corresponding to the escrow encryption key.

8. (Original) The method of claim 1, wherein the escrow encryption key is different from the new public and private keys issued to the addressee.

9. (Original) The method of claim 1, wherein the acknowledgement from the addressee includes an indication of the addressee's name and e-mail address.

10. (Original) The method of claim 1, further comprising the step of:

in response to an address having a public key;

encrypting the package with the addressee's public key;

storing the package;

notifying the addressee of the package;

authenticating a user as the addressee by manipulating a message sent by the addressee encrypted using the addressee's private key; and

transmitting the package to the authenticated addressee in response to authenticating the user as the addressee.

11. (Canceled)

12. (Original) A computer implemented method for securely transmitting an information package to an addressee via a network, the method comprising the steps of:

determining whether the addressee has a public key;

in response to the addressee not having a public key:

encrypting the package with an escrow encryption key;

storing the package in escrow for the addressee;

notifying the addressee of the package in escrow; and

in response to receiving an acknowledgement from the addressee:

issuing new public and private keys to the addressee;

decrypting the package with an escrow decryption key;

re-encrypting the package using the addressee's new public key; and

transmitting the package to the addressee via the network.

13. (Original) The method of claim 12, wherein the step of determining whether the addressee has a public key comprises:

checking a public key directory for a public key of the addressee.

14. (Original) The method of claim 12, further comprising the step of:

storing the addressee's new public key in a public key directory.

15. (Amended) The method of claim 12, wherein the step of transmitting the package comprises the sub-steps of:

authenticating the user as the addressee using a digital signature of addressee; and

transmitting the package to the authenticated user via the network.

16. (Original) The method of claim 12, further comprising the step of:

decrypting the package using he addressee's new private key.

17. (Amended) A system for securely transmitting an information package to an addressee via a network, the system comprising:

a directory interface adapted to check a directory to determine whether the addressee has a public key;

an escrow manager, coupled to the directory interface, adapted to provide an escrow encryption key for encrypting the package;

an encryption module, coupled to the escrow key manager, adapted to encrypt the package with the escrow encryption key;

a computer-readable medium, coupled to the encryption module, adapted to store the package in escrow for the addressee;

a notification module, coupled to the computer-readable medium, adapted to send a notification to the addressee via the network;

a key registration module, coupled to the notification module, adapted to issue, in response to the addressee

acknowledging the notification, new public and private keys to the addressee; and

a transmission module, coupled to the key registration module and to the computer-readable medium, adapted to transmit the package to the addressee via the network in response to successful decryption of a message sent by addressee using the new public key of addressee.

18. (Original) The system of claim 17, further comprising:

a directory coupled to the directory interface, adapted to store a public key of at least one addressee.

19. (Amended) The ~~method~~ system of claim 18, wherein the key registration module is further adapted to store the addressee's new public key in the directory.

20. (Original) The system of claim 17, wherein the notification module is adapted to send one of an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification.

21. (Original) The system of claim 17, wherein the escrow key manager is adapted to provide an escrow decryption key, the system further comprising:

a decryption module, couple to the transmission module, adapted to decrypt the package using the escrow decryption key.

22. (Original) The method of claim 21, wherein the escrow encryption key and the escrow decryption key comprise one of symmetric keys and asymmetric keys.

23. (Original) The system of claim 17, wherein the directory interface and the encryption module are each adapted to operate within a sending system; wherein the computer-readable medium, the notification module, and the transmission module are each adapted to operate within a server system; and
wherein the key registration module and the decryption module are each adapted to operate within a receiving system.

24. (Original) The system of claim 23, wherein the key registration module is received by the receiving system as an attachment to a notification.

25. (Original) The system of claim 23, wherein the key registration module is received by the receiving system by following a hyperlink in a notification.

26. (Original) The system of claim 23, wherein the transmission module within the server system is adapted to transmit the package in escrow to the decryption module within the receiving system; and wherein the decryption module within the receiving system is adapted to receive the package from the transmission module, receive an escrow decryption key manager, and decrypt the package with the escrow decryption key.

27. (Amended) The system of claim 23, wherein the transmission module within the server system is adapted to receive an escrow decryption key from the escrow key ~~manger~~ manager, decrypt the package in escrow using the escrow decryption key, receive the addressee's public key from a directory, re-encrypt the package

using the addressee's public key, and transmit the package to the decryption module within the receiving system; and wherein the decryption module within the receiving system is adapted to receive the package from the transmission module, retrieve the addressee's private key from the key registration module, and decrypt the package using the addressee's private key.

a1

28. (Amended) In a computer-readable medium, a computer program product for securely transmitting an information package to an addressee via a network, the computer-readable medium comprising program code adapted to perform the steps of:

determining whether the addressee has a public key;

in response to the addressee not having a public key;

encrypting the package with an escrow encryption key;

storing the package in escrow for the addressee;

notifying the addressee of the package in escrow; and

in response to receiving an acknowledgement from the addressee:

~~issuing~~ transmitting a new public and private keys generation module to the addressee;

issuing new public and private keys at addressee's location; and

contingent upon authentication of the addressee based on a message sent by addressee subsequent in time to the acknowledgement received from the addressee, transmitting the package to the addressee via the network.

29. (New) The method of claim 1, wherein said step of authentication of the addressee includes the sub-steps of:

the addressee encrypting a message using addressee' private key;

the addressee sending said private-key encrypted message to the sender;

the sender decrypting said private-key encrypted message using addressee's public key;

the sender authenticating the addressee based on the content of the decryption of said private-key encrypted message.

30. (New) The method of claim 1, wherein said step of authentication of the addressee includes the sub-steps of:

the addressee requesting registration with a certificate authority;

the certificate authority registering the addressee subsequent to verifying at least one of the addressee's name, address, telephone number, e-mail address;

the certificate authority generating at least a public key associated with the addressee;

the certificate authority making the public key available for use by the sender; and

the sender authenticating the addressee based on decryption of a message using the public key.

Status

Claim 11 has been cancelled by the present amendment and claims 29 and 30 have been added. Independent claims 1 with claims 2-10, 29 and 30 depending therefrom, independent claim 12 with claims 13-16, independent claim 17 with claims 18-27, and independent 28 will remain for further consideration.

The claims in this application have been revised to voluntarily further clarify Applicant's unique invention. Applicant maintains that the claims as filed were patentable over the art of record. However, to expedite issuance of this application, reconsideration of the claims in light of the amendments and for the following reasons is respectfully requested.

Interview Summary

The Applicant respectfully thanks the Examiner for extending the courtesy of the interview. The Examiner and Applicant discussed proposed amendments to the claims. The prior art discussed included Smith and Vazana. No agreement was reached as to the allowability of the claims.

35 U.S.C. § 103

Claim 1 now recites the additional step of authenticating the addressee before releasing a package to the addressee. A secured system is only as good as its weakest link. The further step of verifying an addressee prior to sending a package held for the

addressee eliminates a potential vulnerability to the system and is not addressed by Smtih. The Smith invention sends a package encrypted by a "secret" key or a "public key" as soon as the public key is received. As required by the claims, the current invention requires the further step of verified authentication of the addressee. This is not cured by Vazana, who is a general minimal secure system for holding a package. There is no incentive to add a Vazana type post office to Smith, because the same purpose of holding a package is already performed by Smith, there is no teaching of a redundant holding system, and even if there were, there is no separate authentication as required by the claims.

Claims 2-10, 29 and 30 should be allowed for at least the same reasons. Additionally claims 5, 10, 29 and 30 require specific types of authentication based on a digital signature and/or a public key of the addressee. These are not addressed by Smith or Vazana and further define the claims over the art of record.

Likewise, claim 17 requires a subsequent verification of the addressee after receipt of the public key, and for the same reasons claims 17-27 should be allowed over the art of record.

In the same way, claim 28 requires subsequent authorization of the addressee after receipt of the public key for additional security. Claim 28 also requires that the notification sent to the addressee include a public keys generation module as opposed to the URL sent in the notification of Smith to prevent IP address duping as is currently a problem, where the URL will appear to be a legitimate address (e.g., http://amazon.com), but the hyperlink underlying IP address actually takes the browser to an unrelated page to steal

vital information from the addressee. For at least these reasons, claim 28 should be allowed.

Claim 12 as originally filed requires that the package held in escrow be unencrypted and re-encrypted with the addressee's public key, once the public key is defined. Again, this helps ensure that the package is never unencrypted to eliminate any vulnerabilities in the system. This is nowhere addressed in Smith or Vazana. Although with reference to claim 27, the Examiner states on page 13 that the "delivery server may decrypt the document using the secret key and alternatively re-encrypt the document (col. 6, lines 3-5) using the recipient's public key" (p. 13), this is respectfully a misreading of Smith. The document encrypted by the public key is never encrypted by the escrow key. See Col. 5, lines 31-39 where Smith explains that the document is not encrypted to minimize processing time, "In an alternative, equally preferred embodiment of the invention, the sender does not encrypt the document until the public key has been received." Nowhere does Smith provide for a document to be unencrypted by the sender and re-encrypted with the public key for security. For at least these reasons, claim 12 and dependent claims 13-16 should be allowed over the art of record.